

What Is Claimed Is:

1. An apparatus for managing access for an extranet, comprising:
 - a plurality of domain web server, to which a plurality of users are subscribed,
 - 5 an AA server for managing access authentication and authorization for the domain web server,
 - an authority information storing module, and
 - a user web browser interconnected with the AA server and the domain web server,
 - wherein the AA server comprises an AA module playing a role of authentication
 - 10 and authorization; an ACL cache control module for synchronizing ACL caches of the respective domain web server with the AA server; an encryption module for encrypting AA cookies to be given to the users; and a schema provider and user provider for providing an operation system independent of the authority information storing module,
 - wherein the domain web server comprises an AA module for checking, by using
 - 15 the ACL cache, whether the user accesses; an ACL cache which is delivered from the AA server; a decryption module for decrypting the encrypted AA cookies; and a module for processing a resource request from the user web browser,
 - wherein the domain web server checks the user authority by using ACL information, respectively, and produces the encrypted Role information cookie, this cookie
 - 20 signal being authenticated in the AA server 300, and, after authentication, Role, ACL, and ACE information is stored in the authority information storing module.
2. A method of managing access for an extranet, performed in the apparatus which comprises the elements in claim 1, the method comprising the steps of:

a user web browser accessing a domain web server,
an AA module of the domain web server confirming access authority of the user web browser,

the user web browser requesting the authentication from the AA module of the AA
5 server,

the AA module of the AA server referring a schema provider to the authority,
the schema provider referring an authority information storing module to a site and delivering the referred result to a user provider, and

the user provider referring the authority information storing module to the user
10 authority to make authentication and set user authority, and transmitting the information to the user web browser.

3. The method of claim 2, further comprising a user authority changing step comprising:

15 if the user web browser requests the service enlisting or quitting, the resource request processing module of the domain web server requesting the AA module of the AA server to enlisting/quitting,

the AA module changing the user authority information and sending the information to the user provider,

20 the user provider updating the user information by sending the changed information to the authority information storing module,

the AA module reporting to the resource request processing module that the user information was changed, such that the user is informed that the enlisting/quitting process is completed.

4. The method of claim 2, further comprising

an ACL initialization step comprising: the AA module of the domain web server requesting the ACL cache control module of the AA server to the ACL cache; and the ACL
5 cache control module referring the ACL cache from the authority information storing module and delivering the referred data to the AA module of the domain web server, and

an ACL synchronization step comprising: a supervisor instructing the ACL cache control module of the AA server to change the authority; and the ACL cache control module requesting the authority information storing module to ACL change and the ACL cache of
10 the domain web server to cache synchronization.